Orderbook Dex Design and Architecture

Submission proposal -
https://forum.freeton.org/t/contest-proposal-freeton-dex-architecture-design-proposal/3067/11

General description

Existing centralized exchanges are constant targets of regulatory, hacker and trading attacks (since launch of bitcoin mtgox, bitfinex and okex are to name a few), which lead to millions of losses of their customers and are one of major obstacles in cryptocurrency and blockchain adoption.

Meanwhile there were a lot of attempts to create a truly decentralized exchange (DEX) based on different strategies like liquidity pools (e.g. uniswap, curve and balance) and order-book based (e.g. idex and loopring), not speaking of partially centralized, partially decentralized. For more information on existing approaches have a look at:

1. https://defipulse.com/
2. https://cointelegraph.com/news/the-first-fundamental-study-of-defi-from-ideas-to-mechanisms-to-the-new-finance

Another major trend is an ongoing early adoption of defi instruments which allow for **non-custodian asset allocation**, majorly in ethereum blockchain, which allows users to gain some interest on their crypto assets without entrusting them to centralized counterparties.

Non-custody allocation, trading and settlement are 3 major goals of proposed architecture for DEX design described in this paper. This work proposes order-book based approach.

This paper presents a high-level view of how such a DEX could look like without specifying particular details of implementations as of now in fact a lot of smart contract development is happening in Free TON community.

Technical stack

This work contains technical prerequisites such as:

1. Ability to create working TIP-3 contracts for stable and governance coins (https://forum.freeton.org/t/tip-3-distributed-token-or-ton-cash/64/5)

2. Some implementation of distributed DB functionality on top of free ton (e.g. https://hypercore-protocol.org/), actively discussed in freeton devex sub-gov (https://forum.freeton.org/t/rtdb-hypercore-test-drive/4456)
3. Implementation of bridge to external blockchains like ethereum and bitcoin (e.g. https://forum.freeton.org/t/contest-ethereum-freeton-bridge-design-and-architecture/2945)
4. Any wallet with support for TIP-3 contracts and ability to work with distributed DB.
5. Existing of external oracles to provide real-time external data to the network like prices of external tokens or fiat currencies.
6. Timer smart contract (https://devex.gov.freeton.org/proposal?proposalAddress=0:91ea1dcdfbaa2d9f869e07a04516addd8752eecd307157e8d4012e1a934094be)

Glossary

1. **CEX** - centralized exchange (e.g. binance, bitfinex, etc)
2. **DEX** - decentralized non-custody exchange
3. **DDB** - decentralized database on top of free ton blockchain
4. **External token (ET)** - any token outside free ton blockchain (e.g. bitcoin, ethereum, etc)
5. **TON Crystal token (TCT)** - original free TON crystal token
6. **Governance token (GT)** - token used to govern all changes to DEX protocol, fees, rewards, contract implementations, etc
7. **Collateral token (CT)** - token usually outside free ton blockchain used as collateral for token inside free ton blockchain.
8. **Stablecoin (SC)** - any TIP-3 token representing an asset inside or outside free ton blockchain
9. **Backed stablecoin (BSC)** - stablecoin backed by some external token, like bitcoin or ethereum (e.g. WBTC on ethereum chain or DAI as in one of ethereum liquidity pools)
10. **Non-backed stablecoin (NBSC)** - stablecoin issued on top free ton blockchain, governed by governance token and not backed by anything like in BSC
11. **Trading pair (TP)** - any pair on top of free ton blockchain (TCT vs GT, TCT vs SC, GT vs NBSC etc) representing set of unique order-books
12. **Order book (OB)** - a group of orders stored in DDB, used to store orders from users
13. **Matching** - a process of matching orders in order book which promotes the exchange of tokens.
14. **Settlement** - a process of settling tokens from user to order book or vice versa, this process also works for BSC when depositing or withdrawing external tokens.
15. **Clearance** - a procedure to match, settle and clean existing TP OBs, the novelty of described approach is that it is done in atomic non-custody distributed fashion unlike in many of existing CEXes and DEXes.
16. **Interest** - yield paid on top of GT, BSC and NBSC, a common approach in CEXes and DEXes of rewarding users for holding the assets within the custody or network
17. **Clearance cycle** - is a parameter regulating how often clearing is happening

18. **Independent automated market maker (IAMM)** - smart contracts which regulate the clearance and distribution of fees and rewards for each particular TP OB
19. **Liquidity pool (LP)** - usually TP LP, specifying tokens which are held by the network in segregated LPs for each SC. As we'll see later BSC LPs and NBSC LPs have a very different nature and regulation.
20. **Seigniorage** - process of minting new tokens for NBSC and GT, which is used both as an economic way of pegging the token to its true market value and way of paying dividends to token holders and liquidity providers
21. **Oracle** - external or internal smart contract, providing market price for an asset or a group of assets

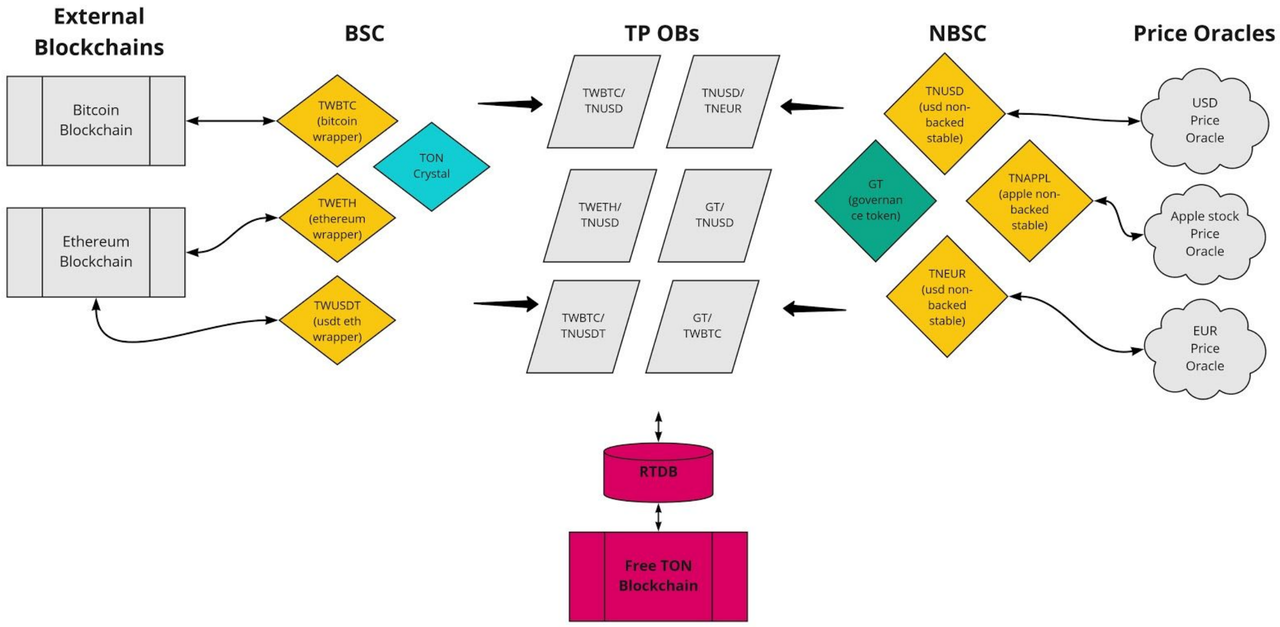
DEX parameters

There are several parameters on dex that regulate overall function and economy of the DEX:

1. wrapper fee (default and per BSC) - fee for wrapping/unwrapping tokens from external chains
2. order fee (default and per TP OB) - fee for putting the order in the order book, necessary to control the flooding of order book, can be default or specific for a particular TP
3. transaction fee (default and per TP OB) - transaction fee taken from each instrument of TP OB pair when distributed matching happenx.
4. clearance cycle - parameter regulating how often clearance happens on the network
5. GT yield (default and per token) - yielding of governance token to stimulate liquidity providers depending on the token users hold
6. NBSC delta rate - rate of seigniorage of NBSC for pegging its value, algorithm will be described later, can be default or specific for NBSC

DEX general architecture

The general architecture is presented on the picture below



The main idea of the proposed architecture is to have two types of tokens, backed up by some liquid asset and non-backed.

With wrapped it's pretty straightforward users pay *wrapper fee*, the default might equal let's say 0.05% with potential to be set higher let's say 0.1% for slow and expensive networks like Bitcoin. These parameters as others will be regulated by governance token and standard SMV (soft majority voting) mechanism used in Free TON network.

With non-backed stable coins (NBSC) DEX governance may launch any arbitrary token with unlimited liquidity and price pegged to some real external price like USD, EUR, any fiat currency, stock prices like Apple, Google, Oil Index price, etc. In a lot of ways it resembles CFD broker contracts (https://en.wikipedia.org/wiki/Contract_for_difference) and allows users to hedge risks of holding volatile wrapped BSC or Ton Crystals.

DEX algorithm and smart contracts

This section contains a brief description of how the algorithm for wrapping, pegging and trading might work, a more detailed description is to be done on the implementation stage. All algos, smart contract deployment and dex parameters are regulated through the governance token. Economy is to be discussed next in the economy section.

Backed Stablecoins

Different wrapping algorithms are better described in submissions for bridge contracts. But on a high level, some relay network provide an ability for a relatively small *wrapper fee* to lock the token in the external network and to issue the BSC token on Free TON network. Unwrapping works the other way and may include some unwrapper fee or might be free.

Non-Backed Stablecoins

NBSC is the most interesting part here. Like in Basis Protocol (https://www.basis.io/) and Reserve (https://reserve.org/) the proposal is to use the mechanism of seigniorage to peg the price of NBSC to its market value received from a given price oracle. Thus the goal of IAMM is to peg the price of NBSC using price oracles and TP OBs stored on the Free TON network.

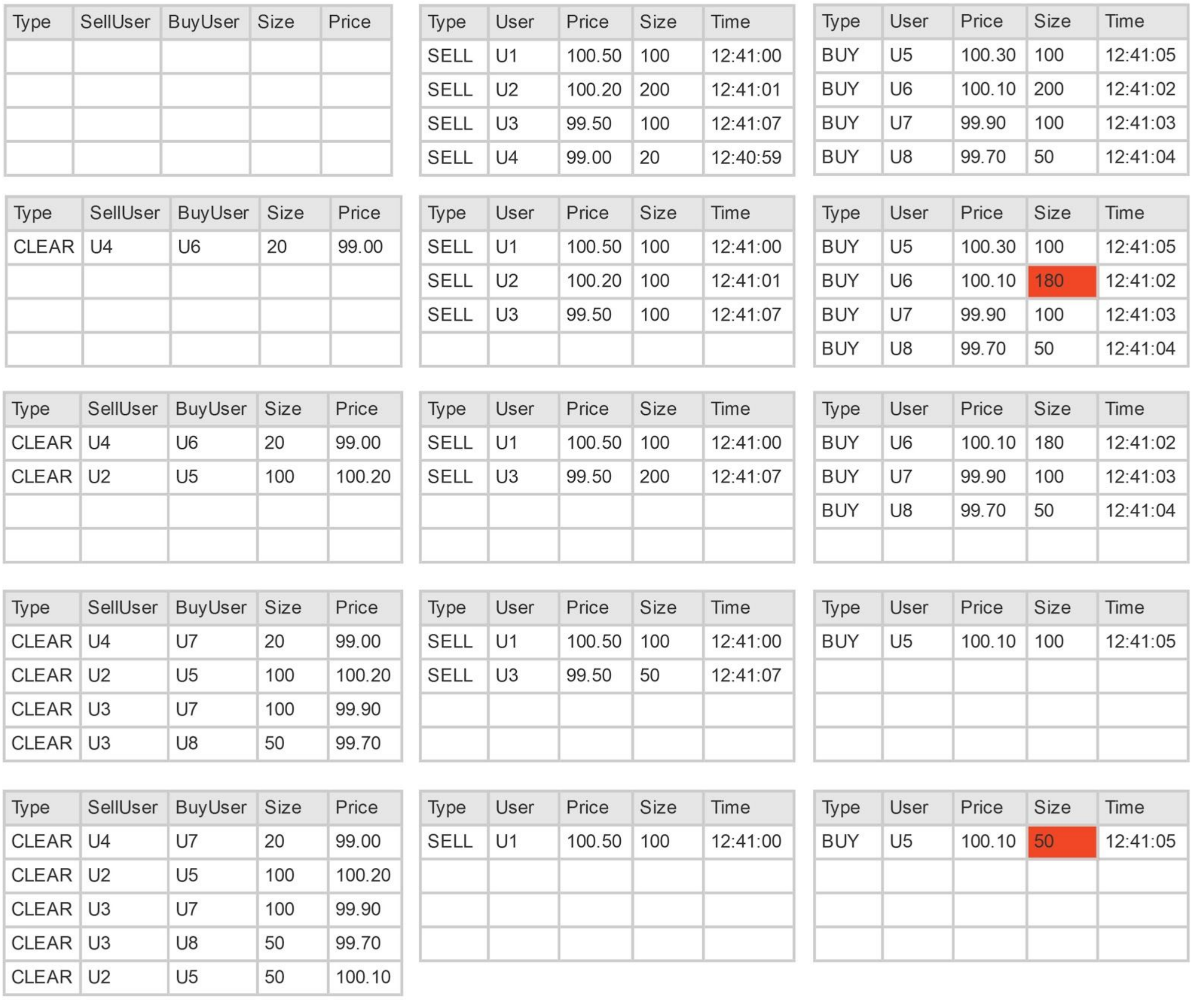
Trading

Every TP OB is stored on FreeTON DDB and is identified by two parameters:

1. Tuple of strings representing BSC and/or NBSC, e.g. {TWBTC, TNUSD} or {TWBTC, TWETH}
2. Contract parameters (or contract specifiaction) like tick size (0 means whole numbers, 10 means all contracts are in size of 10s, 0.01 means size is measured in cents) and maximum order size.
3. A positive integer number, starting from default 0. Numbers more than zero might be used by users to make so-called OTC or Of-order-book deals in similar fashion as it is done on CEXes.

User has an ability to place through TP OB smart contract with given parameter BUY or SELL, amount of being bought or sold (in case of BUYing amount of lower instrument from pair, in case of SELLing amount of upper instrument in pair) and price nominated in ticks according to contract specification. TP OB smart contract checks that all order parameters are correct, the balance of token being bought or sold is sufficient and locks the given token with order fee for this TP and puts into the order book information about the order {UserId, Size, Price}

For every TP OB there is also a so-called Clearance Smart Contract which using the Timer Contract works every X milliseconds according to the clearance cycle DEX parameter. When clearance cycle happens the contract takes all orders sorted by time placement and order prices and cycles through time of placement orders matching it with best possible price similar to a picture shown below



Type	SellUser	BuyUser	Size	Price

Type	User	Price	Size	Time
SELL	U1	100.50	100	12:41:00
SELL	U2	100.20	200	12:41:01
SELL	U3	99.50	100	12:41:07
SELL	U4	99.00	20	12:40:59

Type	User	Price	Size	Time
BUY	U5	100.30	100	12:41:05
BUY	U6	100.10	200	12:41:02
BUY	U7	99.90	100	12:41:03
BUY	U8	99.70	50	12:41:04

Type	SellUser	BuyUser	Size	Price
CLEAR	U4	U6	20	99.00

Type	User	Price	Size	Time
SELL	U1	100.50	100	12:41:00
SELL	U2	100.20	100	12:41:01
SELL	U3	99.50	100	12:41:07

Type	User	Price	Size	Time
BUY	U5	100.30	100	12:41:05
BUY	U6	100.10	180	12:41:02
BUY	U7	99.90	100	12:41:03
BUY	U8	99.70	50	12:41:04

Type	SellUser	BuyUser	Size	Price
CLEAR	U4	U6	20	99.00
CLEAR	U2	U5	100	100.20

Type	User	Price	Size	Time
SELL	U1	100.50	100	12:41:00
SELL	U3	99.50	200	12:41:07

Type	User	Price	Size	Time
BUY	U6	100.10	180	12:41:02
BUY	U7	99.90	100	12:41:03
BUY	U8	99.70	50	12:41:04

Type	SellUser	BuyUser	Size	Price
CLEAR	U4	U7	20	99.00
CLEAR	U2	U5	100	100.20
CLEAR	U3	U7	100	99.90
CLEAR	U3	U8	50	99.70

Type	User	Price	Size	Time
SELL	U1	100.50	100	12:41:00
SELL	U3	99.50	50	12:41:07

Type	User	Price	Size	Time
BUY	U5	100.10	100	12:41:05

Type	SellUser	BuyUser	Size	Price
CLEAR	U4	U7	20	99.00
CLEAR	U2	U5	100	100.20
CLEAR	U3	U7	100	99.90
CLEAR	U3	U8	50	99.70
CLEAR	U2	U5	50	100.10

Type	User	Price	Size	Time
SELL	U1	100.50	100	12:41:00

Type	User	Price	Size	Time
BUY	U5	100.10	50	12:41:05

After no matching is possible all fees are taken by the dex onto the special dex account, and exchange of tokens between users is executed.

During the clearance cycle new orders can be placed into TP OBs but they are not counted in this cycle and are moved to the next cycle appended to final order book from current cycle (see the last state of SELL and BUY tables in the picture)

Pegging

Pegging is the most complicated smart contract and algorithm in DEX after the on-chain matching described in the previous section.
Pegging uses a seigniorage mechanism to stabilize the price asset of non-backed stablecoin.
Pegging is using the same matching algorithm as users. Here comes the IAMMs.
So for each TP OB exists a IAMM smart contract which is feeded with an external price oracle. Price Oracle can be direct and be feeded let’s say with the price of EUR/USD on biggest forex exchange EBS or something or can be synthetic using several EUR/USD data feeds and making an aggregate, or calculating for example price for BTC/RUB using two feeds BTS/USD and USD/RUB. The composition of particular price feeds is decided by the governance.

So here we assume that Oracles are set up and ready to use, moreover we don't insist on oracle to be ultra fast and latency free, here we introduce NBSC delta rate, which regulates once the price in TP OB fluctuates more than given delta, IAMM starts putting enough size in the (oracle market price + delta) range to stabilize the liquidity. The delta shouldn't be too big to be effective in stabilization and not too small to create potential arbitrage opportunities and is decided by governance, the default can be around 1%. This algo resembles a lot into how state central banks inject liquidity to stabilize the price of the state currency in relation to external.

There are 3 possible cases:

1. TP OB, NBSC vs NBSC, e.g. TNEUR/TNUSD, it's the simplest case as there is unlimited supply for both SCs. Let's say that the market price is 1.18, at some point it starts to deviate towards 1.2 inside free TON TP OB due to high demand for TNEUR. Then IAMM as a separate agent should start putting into TNEUR/TNUSD OB orders with sizes let's say 1mEUR at a price around (1.18 + 1% ~ 1.1918). The size of order might be equal to some Seigniorage Order Size SOS, where size = SOS x ADTV, where ADTV is the average daily volume traded on the previous day. If the prices goes below the market value, let's say to 1.17, then IAMM puts enough liquidity from TNUSD pull at price (1.18 - 1% ~ 1.1682)
2. TP OB, BSC vs BSC, e.g. TWBTC/TWETH, here the proposition is to use no IAMM and let the users arbitrageurs, stabilize the liquidity by injecting the unpegged liquidity through a wrapping mechanism, introduced in the previous section.
3. And the most complicated case - BSC vs NBSC, e.g. TWBTC/TNUSD. Let's say the oracle market price is 16000$. If TWBTC/TNUSD starts to unpeg towards 15000$, the solution is easy as in first case at price around 15840 (16000 - 1%) IAMM will start injecting liquidity of TNUSD and buying cheap (compared to oracle market price) TWBTC. If TWBTC/TNUSD starts to unpeg toward unfair 17000$ price (if oracle price of course stays around 16000$) it's harder coz surely DEXs has account with governance tokens and fees paid to it which can be sold or exchanged and used to peg the price of TWBTC down a bit, but those supplies are very limited, another plausible option is to start to make fees asymmetrical, for example in this case of unpegging to 17000$ DEX can start to decrease the order and transaction fees for selling TWBTC and increase the same for buying TWBTC, it should be some variation of logarithimic scale, e.g. each increase in price for 1%, let's say to 16160 (16000 + 1%), should yield a decrease of 0.1% in order and transaction fee for selling TWBTC and increase of 0.1% for buying TWBTC.

DEX economy

So in the previous section there was given a high view architecture of order book based DEX with matching and settlement on chain, independent IAMMs to control the pegging of NBSC, and the governance to regulate numerous parameters in the DEX to provide price stability and maximise utilization of the DEX.
Let's see from the economic perspective how such a DEX can incentivize users to use it for their daily exchange operations and at the same time benefit on the growth of the network in general and exchange in particular.

The basic motivation is obvious, people want to transfer their assets between blockchain depending on their needs and purposes, they want to exchange one asset over their and in best case scenario earn some yield for being involved in this process.
On the other hand a good DEX implementation should ensure the stability of the exchange process, gain some dividends for active users and liquidity providers and provide some governance mechanism for future changes and improvements.

So 2 basic economy mechanics for the proposed solution are:

1. Free TON network is used as backbone infrastructure for efficient smart contract and cheap execution, TON crystal (TC) is used as a gas.
2. Governance token (GT) is used as a token to govern parameters of the DEX and distribute dividends to active users and maintainers.

Next obvious thing is that due to the fact that gas is payed in TC, DEX should have enough liquidity for TON crystal through TP OBs and IAMS for Ton Crystal pair.
Moreover the first X transactions on the network can be rewarded with not just GTs but TON crystals as well through airdrop mechanism for instance.

Another important thing is development and improvement of existing smart contracts and tuning of DEX parameters, all that things in similar fashion to Free TON governance should be done through voting with governance token and SMV contracts.

The basic reward mechanism should reward users with GTs and potentially CTs for:

1. Each trade, similar to cashback where to Y% (another DEX parameter) percent is returned to both liquidity providers.
2. For BSC liquidity providing the cashback should be definitely bigger, up to 2Y% or even more, depending on the need of backed liquidity, this increase should also be governed by GT. DEX like central banks should ensure that there is always a substantial percent of liquidity (yet another governed DEX parameter, by default can equal to about 10-20% like in fractional reserve systems) is held in backed stablecoins through mechanism of rewarding with GT hodlers of BSC, decreasing order and transaction fees for selling BSCs and in worst case scenarios when level of backed coins drop below threshold - increasing of unwrapping fees.

All wrapping, order and trading fees are collected on special DEX account which once in a given period (another DEX parameter, can equal by default to 1 month), distributes a portion of it in form of dividents (DEX parameter, around 10%) to GT token holders. Later on a Liquidity based approach and super-IAMM can be used to automatically trade this funds to provide liquidity for price stabilization and internal arbitrage on the DEX.

Tackling of existing problems

As for problems described in contest proposal for on-chain order-book dex approach they are practically non-existent (their true nature relates more to liquidity based approaches):

1. Frontrunning is impossible due to synchronous matching and settlement algorithm described in Algorithm section

2. No problems with curves as well as everything is done through order book and price oracles insure stability of NBSCs.
3. No impairment loss as all liquidity is separated into different order books and is not mixed up at any place and time.
4. Customized proportion of assets is non-existent here.
5. Scalability of order-book based approach is reached through introducing order fee, which effectively stops users from over-flooding OBs with unnecessary orders and ensures stability of fair trade without frontrunning or flashing orders approaches popular in micro and hft trading.

Contacts

tg @rainblowing
mail rainblowing@me.com